证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2002 09 23

申　请　号：　02 1 42879.4

申请类别：　发明

发明创造名称：　使用请求短消息点播视频节目的视频点播系统及其方法

申　请　人：　国际商业机器公司

发明人或设计人：张健；邵凌；谢东

中华人民共和国
国家知识产权局局长　王景川

2003 年 5 月 12 日

权 利 要 求 书

1. 一种通过短消息来点播视频节目的视频点播方法，所述方法包括：

在用户端生成包含用户请求点播的视频节目在内的请求短消息，该请求短消息至少包括用户身份识别符字段、用户所请求的视频节目的节目识别符字段、以及一认证字段；

向节目提供端发送所生成的请求短消息；

在节目提供端接收所述请求短消息，并对收到的请求短消息进行处理，提取用户身份识别符，使用认证字段验证用户的合法性；

在验证用户合法后，将节目识别符所对应的节目内容从节目提供端发送到用户身份识别符所指示的用户端；以及

在用户端接收所点播的视频节目。

2. 如权利要求 1 所述的视频点播方法，还包括步骤：

从节目提供端向用户端发送包括表明已经收到请求短消息的确认消息在内的应答消息。

3. 如权利要求 1 所述的视频点播方法，还包括步骤：

在用户端将生成的请求短消息中认证字段之外的字段加密；以及

在节目提供端中解密所收到的加密短消息，以提取用户身份识别符和节目识别符。

4. 如权利要求 1 至 3 中任一所述的视频点播方法，其中所述请求短消息还包括：

格式识别符字段，用于规定所述请求短消息的格式；

请求时间字段，用于表示发送所述请求的时间；

播放时间字段，用于表示视频播放的开始时间；

可选字段，其中包含用于更详细地描述所述请求的可选数据；并且

所述认证字段是上述用户身份识别符字段、节目识别符字段、格式识别符字段、请求时间字段、播放时间字段、和可选字段的加密摘要。

5. 如权利要求 4 所述的视频点播方法，其中

所述认证字段按照下述步骤生成：1）采用摘要算法计算除认证字段之外的所有字段的摘要；2）采用加密算法，使用由节目提供端事先唯一分配的对应用户端装置的保密认证密钥对所计算的摘要进行加密；以及

节目提供端执行的所述验证用户的合法性按照下述步骤进行：1）采用摘要算法计算除认证字段之外的字段的摘要；2）采用加密算法，使用其事先唯一分配的对应用户端装置的保密认证密钥对所计算的摘要进行加密，计算出认证字段；3）校验所计算的认证字段与收到的认证字段是否一致。

6. 如权利要求 5 所述的视频点播方法，其中：

如果所述视频节目通过有条件接入系统发送，则内容密钥与所述视频节目一起发送，从而无需单独发送所述应答消息。

7. 如权利要求 5 所述的视频点播方法，其中，如果用户所点播的视频节目需要加密且密钥不通过有条件接入系统发送，则还包括如下步骤：

在节目提供端生成一包含所述视频节目的内容密钥在内的加密应答消息并发送给用户端；

在用户端从所述加密应答消息中解密内容密钥；以及

根据该解密的内容密钥将从节目提供端收到的视频节目解密。

8. 如权利要求 7 所述的视频点播方法，其中所述加密的内容密钥是用由节目提供端事先唯一分配的对应用户端装置的设备密钥加密的，并且所述设备密钥与所述认证密钥可以不同。

9. 一种通过短消息来点播视频节目的视频点播系统，包括：

短消息生成装置，用于接收用户发出的请求，根据用户的请求生成至少包括用户身份识别符字段、用户所请求的视频节目的节目识别符字段、以及一认证字段在内的请求短消息；

短消息发送装置，用于发送短消息生成装置所生成的请求短消息；

节目提供端的请求短消息处理装置，用于接收所述请求短消息，并对收到的请求短消息进行处理，提取用户身份识别符，使用认证字段验证用户的合法性，以及将合法用户所请求的节目的节目识别符发送给视频提供装置；

视频提供装置，用于将节目识别符所对应的节目内容发送到合法用户身份识别符所指示的用户端；以及

用户端的节目播放装置，用于接收视频提供装置所发送的视频节目并播放给用户观看。

10. 如权利要求 9 所述的视频点播系统，其中：

请求短消息处理装置中还包括应答消息生成单元，用于生成向用户端发送的至少包含表明已经收到请求短消息的确认消息在内的应答消息。

11. 如权利要求 9 所述的视频点播系统，其中：

短消息生成装置包括加密单元，用于将生成的请求短消息中除认证字段之外的字段加密；以及

请求短消息处理装置包括解密单元，用于解密所收到的加密的请求短消息。

12. 如权利要求 9 至 11 任一所述的视频点播系统，其中

所述短消息生成装置包括节目信息生成单元，用于生成所述用户身份识别符字段、用户所请求的视频节目的节目识别符字段、以及：

格式识别符字段，用于规定所述请求短消息的格式；

请求时间字段，用于表示发送所述请求的时间；

播放时间字段，用于表示视频播放的开始时间；以及

可选字段，其中包含用于更详细地描述所述请求的可选数据。

13. 如权利要求 12 所述的视频点播系统，其中：

所述短消息生成装置包括认证字段生成单元，用于采用摘要算法计算除认证字段之外的字段的摘要；并采用加密算法，使用由视频提供装置事先唯一分配的对应用户端装置的保密认证密钥对所计算的摘要进行加密，从而生成请求短消息中的认证字段；以及

所述请求短消息处理装置包括验证单元，用于采用摘要算法计算所述用户身份识别符字段、节目识别符字段、格式识别符字段、请求时间字段、播放时间字段、以及可选字段的摘要；并采用加密算法，使用由视频提供装置唯一对应分配给用户端装置的保密认证密钥对所计算的摘要进行加密，从而生成请求短消息中的认证字段；以及校验所计算的认证字段与收到的认证字段是否一致。

14. 如权利要求 13 所述的视频点播系统，其中：

如果所述视频节目通过有条件接入系统发送，则内容密钥与所述视频节目一起发送，从而无需单独发送所述应答消息。

15. 如权利要求 13 所述的视频点播系统，其中，如果用户所点播的视频节目需要加密且密钥不通过有条件接入系统发送，则：

请求短消息处理装置生成一包含所述视频节目的内容密钥在内的加密应答消息并发送给用户端；以及

在用户端的节目播放装置从所述加密应答消息中解密内容密钥，并根据

该解密的内容密钥将从视频提供装置收到的视频节目解密。

16. 如权利要求 15 所述的视频点播系统，其中所述加密的内容密钥是用由节目提供端事先唯一分配的对应用户端装置的设备密钥加密的，并且所述设备密钥与所述认证密钥可以不同。

17. 一种视频点播系统中的短消息生成装置，包括：

接收单元，用于接收用户发出的请求；

节目信息生成单元，用于根据用户的请求生成至少包括用户身份识别符字段、以及用户所请求的视频节目的节目识别符字段在内的节目信息；

认证字段生成单元，用于根据节目信息生成单元所生成的节目信息生成认证字段；以及

输出单元，用于将上述节目信息和认证字段作为请求短消息输出给一短消息发送装置。

18. 如权利要求 16 所述的短消息生成装置，还包括：

加密单元，用于将请求短消息中除认证字段之外的字段加密。

19. 如权利要求 17 或 18 所述的短消息生成装置，其中，所述节目信息生成单元还生成：

格式识别符字段，用于规定所述请求短消息的格式；

请求时间字段，用于表示发送所述请求的时间；

播放时间字段，用于表示视频播放的开始时间；以及

可选字段，其中包含用于更详细地描述所述请求的可选数据。

20. 如权利要求 19 所述的短消息生成装置，其中：

所述认证字段生成单元采用摘要算法计算除认证字段之外的字段的摘要，并采用加密算法，使用事先确定的唯一对应于该短消息生成装置的保密认证密钥对所计算的摘要进行加密。

21. 如权利要求 20 所述的短消息生成装置，其中，所述摘要算法为 MD5 算法，所述加密算法为 3DES 算法。

22. 一种视频点播系统中的短消息生成方法，包括下列步骤：

根据用户的请求生成至少包括用户身份识别符字段、以及用户所请求的视频节目的节目识别符字段在内的节目信息；

根据所生成的节目信息生成认证字段；以及

将上述节目信息和认证字段作为请求短消息输出给一短消息发送装置。

23. 如权利要求 22 所述的短消息生成方法，还包括将请求短消息中除认证字段之外的字段加密的步骤。

24. 如权利要求 22 或 23 所述的短消息生成方法，其中，所生成的节目信息还包括：

格式识别符字段，用于规定所述请求短消息的格式；

请求时间字段，用于表示发送所述请求的时间；

播放时间字段，用于表示视频播放的开始时间；以及

可选字段，其中包含用于更详细地描述所述请求的可选数据。

25. 如权利要求 24 所述的短消息生成方法，其中所述认证字段生成步骤包括下列步骤：

采用摘要算法计算除认证字段之外的字段的摘要；以及

采用加密算法，使用事先唯一确定的保密认证密钥对所计算的摘要进行加密。

26. 如权利要求 25 所述的短消息生成方法，其中，所述摘要算法为 MD5 算法，所述加密算法为 3DES 算法。

27. 一种视频点播系统中的请求短消息处理装置，包括：

接收单元，用于接收用户所发送的请求短消息；

提取单元，用于从接收单元所收到的请求短消息中提取用户身份识别符；

验证单元，用于根据接收单元所收到的请求短消息中的认证字段，验证由提取单元提取的用户身份识别符所标识的用户的合法性；以及

输出单元，用于输出合法用户所请求的节目的节目识别符。

28. 如权利要求 27 所述的请求短消息处理装置，还包括：

解密单元，用于解密所收到的加密的请求短消息。

29. 如权利要求 27 或 28 所述的请求短消息处理装置，其中：

所述验证单元采用摘要算法计算所收到的请求短消息中除认证字段之外的字段的摘要；采用加密算法，使用与用户端唯一对应分配的保密认证密钥对所计算的摘要进行加密，从而生成请求短消息中的认证字段；以及校验所计算的认证字段与收到的认证字段是否一致。

30. 如权利要求 29 所述的请求短消息处理装置，其中，所述摘要算法为 MD5 算法，所述加密算法为 3DES 算法。

31. 如权利要求 30 所述的请求短消息处理装置，还包括：

应答消息生成单元，用于生成向用户端发送的至少包含表明已经收到请求短消息的确认消息在内的应答消息。

32. 一种视频点播系统中的请求短消息处理方法，包括下列步骤：

接收用户所发送的请求短消息；

从所收到的请求短消息中提取用户身份识别符；

根据所收到的请求短消息中的认证字段，验证所提取的用户身份识别符标识的用户的合法性；以及

输出合法用户所请求的节目的节目识别符。

33. 如权利要求 32 所述的请求短消息处理方法，还包括将所收到的加密的请求短消息解密的步骤。

34. 如权利要求 32 或 33 所述的请求短消息处理方法，其中所述验证步骤包括下列步骤：

采用摘要算法计算所收到的请求短消息中除认证字段之外的字段的摘要；

采用加密算法，使用与用户端唯一对应分配的保密认证密钥对所计算的摘要进行加密，从而生成请求短消息中的认证字段；以及

校验所计算的认证字段与收到的认证字段是否一致。

35. 如权利要求 34 所述的请求短消息处理方法，其中，所述摘要算法为 MD5 算法，所述加密算法为 3DES 算法。

36. 如权利要求 35 所述的请求短消息处理方法，还包括生成向用户端发送的至少包含表明已经收到请求短消息的确认消息在内的应答消息并输出的步骤。

说　明　书

使用请求短消息点播视频节目的视频点播系统及其方法

技术领域

本发明涉及视频点播（VOD，Video-on-Demand），更具体地说，涉及使用具有认证功能的请求短消息点播视频节目的视频点播系统及其方法。

背景技术

在 VOD 系统中，必须具有用于将用户请求发送给 VOD 服务供应商的返回信道。在传统的 VOD 系统中，用户通常通过因特网或者有线电视双向电缆的反向信道来进行视频点播，如美国专利 US5945987“Interactive Entertainment Network System and Method for Providing Short Sets of Preview Video Trailers”、美国专利 US5973722 “Combined Digital Audio/Video on Demand and Broadcast Distribution System”、美国专利申请 US2002/0019984A1 “Headend Cherrypicker with Digital Video Recording Capability” 等所公开的系统。

但是，在用户使用因特网不方便、以及没有有线电视双向电缆的反向信道的情况下，用户只能通过电话进行视频点播。

而且，在使用上述因特网或者有线电视双向电缆的反向信道进行视频点播时，不仅成本和费用较高，用户使用也不方便。在通过电话点播视频节目的情况下，其安全性和保密性也难以得到很好的保证。

解决上述问题的一种办法是通过与 VOD 系统的请求处理装置非直接连接的装置发送短消息给请求处理装置来实现视频节目的点播。短消息不仅可以实现人和人之间的远距离沟通，而且费用低廉、便于计算机处理，所以在当前的移动通信系统和人们的社会生活中得到了普遍应用。此外，应用短消息来作为反向信道还省去了改造有线电视的电缆为双向电缆、以及为用户的接收装置加装因特网接入单元和功能等不仅烦琐而且成本很高的工作。

但是，传统的短消息应用也存在明显的不足，仅限于交换一些保密性要求不高的信息。这是由于用户身份只能通过电话号码来验证，如果一个家庭拥有多部手机，并且每一个家庭成员都可以使用任何一部手机来发送短消息，则对于 VOD 系统来说，电话号码将不再是合适的身份识别符。另外，使用电

话号码作为身份识别符来验证也是不安全的，比如可以盗用他人的电话号码来发送短消息进行视频点播。此外，当前的短消息都是明文发送的，没有经过加密，所以其安全性和保密性也难以得到保证。随着黑客（hacker）技术的不断发展、识别用户手机的ID（身份标识符）并盗用已经不是非常困难的事情。因此，如果使用手机的短消息进行视频点播，将很不安全。

发明内容

有鉴于上述情况，本发明的目的是提供一种通过具有认证功能的请求短消息来点播视频节目的视频点播方法，从而可以方便安全地实现远程视频点播，而且成本低廉、保密性强。

本发明的另一目的是提供一种通过具有认证功能的请求短消息来点播视频节目的视频点播系统，从而可以方便安全地实现远程视频点播，而且成本低廉、保密性强。

本发明的再一目的是提供一种生成上述具有认证功能的请求短消息的短消息生成装置及其生成方法。

本发明的又一目的是提供一种对上述具有认证功能的请求短消息进行处理的请求短消息处理装置及其处理方法。

为了实现上述目的，本发明提供了一种通过短消息来点播视频节目的视频点播方法，所述方法包括：在用户端生成包含用户请求点播的视频节目在内的请求短消息，该请求短消息至少包括用户身份识别符字段、用户所请求的视频节目的节目识别符字段、以及一认证字段；向节目提供端发送所生成的请求短消息；在节目提供端接收所述请求短消息，并对收到的请求短消息进行处理，提取用户身份识别符，使用认证字段验证用户的合法性；在验证用户合法后，将节目识别符所对应的节目内容从节目提供端发送到用户身份识别符所指示的用户端；以及在用户端接收所点播的视频节目。

在根据本发明的上述视频点播方法中，如果用户所点播的视频节目需要加密，则还生成一包含所述视频节目的内容密钥在内的加密应答消息并发送给用户端，从而在用户端可以从所述加密应答消息中解密内容密钥，并根据该内容密钥将从节目提供端收到的视频节目解密。

根据本发明的另一方面，提供一种通过短消息来点播视频节目的视频点播系统，包括：短消息生成装置，用于接收用户发出的请求，根据用户的请

求生成至少包括用户身份识别符字段、用户所请求的视频节目的节目识别符字段、以及一认证字段在内的请求短消息；短消息发送装置，用于发送短消息生成装置所生成的请求短消息；节目提供端的请求短消息处理装置，用于接收所述请求短消息，并对收到的请求短消息进行处理，提取用户身份识别符，使用认证字段验证用户的合法性，以及将合法用户所请求的节目的节目识别符发送给视频提供装置；视频提供装置，用于将节目识别符所对应的节目内容发送到合法用户身份识别符所指示的用户端；以及用户端的节目播放装置，用于接收视频提供装置所发送的视频节目并播放给用户观看。

在根据本发明的上述视频点播系统中，如果用户所点播的视频节目需要加密，则请求短消息处理装置还生成一包含所述视频节目的内容密钥在内的加密应答消息并发送给用户端；并且，在用户端的节目播放装置则可以从所述加密应答消息中解密内容密钥，并根据该内容密钥将从视频提供装置收到的视频节目解密。

根据本发明的另一方面，提供一种视频点播系统中的短消息生成装置，包括：接收单元，用于接收用户发出的请求；节目信息生成单元，用于根据用户的请求生成至少包括用户身份识别符字段、以及用户所请求的视频节目的节目识别符字段在内的节目信息；认证字段生成单元，用于根据节目信息生成单元所生成的节目信息生成认证字段；以及输出单元，用于将上述节目信息和认证字段作为请求短消息输出给一短消息发送装置。

根据本发明的再一方面，提供一种视频点播系统中的短消息生成方法，包括下列步骤：根据用户的请求生成至少包括用户身份识别符字段、以及用户所请求的视频节目的节目识别符字段在内的节目信息；根据所生成的节目信息生成认证字段；以及将上述节目信息和认证字段作为请求短消息输出给一短消息发送装置。

根据本发明的另一方面，提供一种视频点播系统中的请求短消息处理装置，包括：接收单元，用于接收用户所发送的请求短消息；提取单元，用于从接收单元所收到的请求短消息中提取用户身份识别符；验证单元，用于根据接收单元所收到的请求短消息中的认证字段，验证由提取单元提取的用户身份识别符所标识的用户的合法性；以及输出单元，用于输出合法用户所请求的节目的节目识别符。

根据本发明的再一方面，提供一种视频点播系统中的请求短消息处理方

法，包括下列步骤：接收用户所发送的请求短消息；从所收到的请求短消息中提取用户身份识别符；根据所收到的请求短消息中的认证字段，验证所提取的用户身份识别符标识的用户的合法性；以及输出合法用户所请求的节目的节目识别符。

采用根据本发明的视频点播系统及其方法、短消息生成装置及其生成方法、以及请求短消息处理装置及其处理方法，不仅方便可靠、而且简单易行，免却了对现有通过有线电缆进行视频点播的系统的双向改造，也方便了那些没有因特网接入的用户。同时，其保密性也得到了保证，为运营商提供了良好的运行环境。

附图说明

通过以下借助附图的详细描述，将会更容易地理解本发明，其中相同的标号指定相同结构的单元，并且在其中：

图 1 是根据本发明优选实施例的视频点播系统的方框图；

图 2 是根据本发明的优选实施例的图 1 中短消息生成装置的详细方框图；

图 3 是根据本发明的优选实施例的表示图 2 的短消息生成装置所生成的请求短消息的格式的图；

图 4 是根据本发明的优选实施例的图 1 中请求短消息处理装置的详细方框图；以及

图 5 是根据本发明优选实施例的视频点播方法的流程图。

具体实施方式

下面将结合附图详细描述本发明的优选实施例。在下面的描述中，现有 VOD 系统中公知的单元将不再详细描述，以免以不必要的细节混淆本发明。

图 1 是根据本发明优选实施例的视频点播系统的方框图。如图 1 所示，根据本发明的实施例的视频点播系统包括：用户端短消息生成装置 12，用于接收用户发出的请求，根据用户的请求生成至少包括用户身份识别符字段、用户所请求的视频节目的节目识别符字段、以及一认证字段在内的请求短消息；短消息发送和接收装置 14，用于发送短消息生成装置所生成的请求短消息、并用于接收从节目提供端发送的包括通知收到请求短消息的确认消息在内的应答消息；节目提供端的请求短消息处理装置 15，例如，请求处理服务

器，用于接收所述请求短消息，并对收到的请求短消息进行处理，提取用户身份识别符，使用认证字段验证用户的合法性，以及将合法用户所请求的节目的节目识别符发送给诸如视频点播服务器之类的视频提供装置 16；视频提供装置 16，用于将节目识别符所对应的节目内容发送到合法用户身份识别符所指示的用户端；以及用户端的节目播放装置 13，用于接收视频提供装置 16 所发送的视频节目并播放给用户观看。

在该系统中，用于发送短消息的短消息发送和接收装置 14 一般是当前非常普及的移动电话。因此，不仅方便了不便应用因特网的用户，而且省去了对现有有线电视电缆的双向改造，从而有利于视频点播业务的普及和发展。

当然，在该系统中也可以使用任何其它能够发送短消息的装置作为短消息发送和接收装置 14。比如，在某些城市已经开通了通过固定电话发送短消息的业务，因此也可以通过固定电话来发送短消息。

另外，短消息生成装置 12 与短消息发送和接收装置 14 之间的连接，既可以是无线连接，也可以是有线连接。

由于视频点播系统需要较高的安全可靠性，而且在提供视频点播业务的服务方必须能够验证点播用户是否为合法用户，但是现在常用的短消息却是明文发送的，非常易于仿冒，因此，采用传统的短消息格式，其安全性和用户合法性的验证无法实现。

根据本发明的短消息生成装置 12 则可以生成保密的且可以验证用户合法性的具有认证功能的短消息。下面详细说明根据本发明的短消息生成装置 12 及其生成的加密短消息的格式。

图 2 示出根据本发明的优选实施例的短消息生成装置 12 的详细方框图。如图 2 所示，根据本发明优选实施例的短消息生成装置 12 包括：接收单元 201，用于接收用户发出的点播请求；节目信息生成单元 202，用于生成用户身份识别符字段、用户所请求的视频节目的节目识别符字段、规定所述请求短消息的格式的格式识别符字段、表示发送所述请求的时间的请求时间字段、以及表示视频播放的开始时间的播放时间字段等有关用户点播的节目信息；认证字段生成单元 203，用于采用如 MD5 的摘要算法计算上述字段的摘要，并采用如 3DES 的加密算法，使用由视频提供装置事先唯一分配的对应于该短消息生成装置 12 的保密认证密钥对所计算的摘要进行加密，从而生成认证字段；输出单元 204，用于将上述节目信息和认证字段作为请求短消息输出

给短消息发送和接收装置 14。

为了更加安全起见，该短消息生成装置 12 还可以配置加密单元（图中未示出），用于将生成的请求短消息中除认证字段之外的字段加密，从而使有关用户点播的节目信息更加安全可靠。此时、认证字段可以是通过对上述加密的其它各字段计算摘要、并使用保密认证密钥加密得到的字段。

此外，为了便于发送、接收以及与现有短消息统一，所有字段的长度的和最好不大于 100 字节。所述请求短消息还可以包括不大于 40 字节的可选字段，其中包含用于更详细地描述所述请求的可选数据。

由本发明的短消息生成装置 12 所生成的请求短消息的优选格式如图 3 所示。各个字段说明如下。

格式识别符字段，8 比特，规定该请求短消息所使用的格式；

用户身份识别符字段，32~64 比特，用于识别用户和短消息生成装置；

节目识别符字段，长度在 20 至 72 字节之间可变，用于表示用户所请求的视频节目；

请求时间字段，32 比特，用于表示发送请求时间；

播放时间字段，32 比特，用于表示视频播放的开始时间，例如可以是“立即开始”；

可选字段，不大于 40 字节，其中包含用于更详细地描述所述请求的可选数据；以及

认证字段，128 比特，为上述所有字段的加密摘要，可以由请求短消息处理装置 15 校验以证实发出该请求短消息的用户为合法用户，从而使视频提供装置 16 仅将节目内容发送到合法用户端。

与短消息生成装置 12 相对应，在提供视频点播服务的一端的请求短消息处理装置 15 中必须能够解密由短消息发送和接收装置 14 发送的短消息生成装置 12 所生成的具有认证功能的请求短消息。图 4 示出根据本发明优选实施例的请求短消息处理装置 15 的详细方框图。

如图 4 所示，根据本发明优选实施例的请求短消息处理装置 15 包括：接收单元 401，用于接收短消息发送和接收装置 14 所发送的请求短消息；提取单元 402，用于对收到的请求短消息进行处理，提取用户身份识别符等有关节目的信息；验证单元 403，用于采用如 MD5 的摘要算法计算提取单元 402 所提取的所述用户身份识别符字段、节目识别符字段、格式识别符字段、请

求时间字段、和播放时间字段的摘要，并采用如 3DES 的加密算法，使用由视频提供装置 16 唯一对应分配给用户端的短消息生成装置 12 的保密认证密钥对所计算的摘要进行加密，从而生成请求短消息中的认证字段，以及校验所计算的认证字段与收到的认证字段是否一致；应答消息生成单元 404，用于生成向短消息发送和接收装置 14 发送的至少包含表明已经收到请求短消息的确认消息在内的应答消息；以及输出单元 405，用于将应答消息生成单元 404 所生成的确应答消息通过短消息发送和接收装置 14 传送给节目播放装置 13，或者在视频节目通过有条件接入系统发送的情况下，将该应答消息输出给视频提供装置 16，由视频提供装置 16 将该应答消息与加密的视频内容一起发送给节目播放装置 12。同时，输出单元 405 还将提取单元所提取的诸如用户身份识别符、节目识别符、格式识别符、请求时间、和播放时间等有关节目的信息输出给视频提供装置 16，以便视频提供装置 16 仅提供给合法用户所点播的视频节目。

应答消息最简单的格式是在上述请求短消息的基础上增加一包含表示所述加密的内容密钥的密钥字段。该密钥字段的长度不大于 128 比特。

其中，所述加密的内容密钥是用与视频提供装置 16 唯一对应分配的短消息生成装置的唯一身份识别符相对应的设备密钥加密的。

并且，由于公知的加密常识，同一密钥的使用次数越多，其保密性越难以得到保证，因此尽管不是必需的，但是最好设备密钥与认证密钥不同。

此外，用户端的节目播放装置 12 中还应包括应答消息解密单元，用于从收到的加密应答消息中解密内容密钥，根据该解密的内容密钥将从视频提供装置 16 收到的视频节目解密。

另外，如果在短消息生成装置 12 中配置了加密请求短消息的加密单元，则在请求短消息处理装置 15 中需要配置解密单元（图中未示出），用于解密从短消息发送和接收装置 14 所收到的加密的请求短消息。

以上所述为根据本发明优选实施例的视频点播系统。下面将描述在上述视频点播系统中用户点播视频节目的方法。

在根据本发明的视频点播方法中，首先在用户端生成包含用户请求点播的视频节目在内的请求短消息，该请求短消息至少包括用户身份识别符字段、用户所请求的视频节目的节目识别符字段、以及一认证字段。然后，向节目提供端发送所生成的请求短消息。在节目提供端接收所述请求短消息，并对

收到的请求短消息进行处理，提取用户身份识别符，使用认证字段验证用户的合法性。接着，在验证用户合法后，将节目识别符所对应的节目内容从节目提供端发送到用户身份识别符所指示的用户端。随后，在用户端接收所点播的视频节目。

下面将结合图 5 详细描述在上述视频点播系统中所采用的上述视频点播方法，以便实现用户通过具有认证功能的短消息方便地点播自己所喜好的节目，而又不会增加额外的开销。

图 5 是根据本发明优选实施例的视频点播方法的流程图。如图 5 所示，在用户发出命令点播自己想观看的节目之后，在步骤 SP1，短消息生成装置 12 接收该命令，并根据用户的命令生成包含用户请求点播的视频节目的具有认证功能的请求短消息，该请求短消息包括规定请求短消息的格式的格式识别符字段、表示用户身份的用户身份识别符字段、表示用户所请求的视频节目的节目识别符字段、表示发送请求时间的请求时间字段、表示视频播放的开始时间的播放时间字段、其中包含用于更详细地描述所述请求的可选数据的可选字段、以及作为上述字段的加密摘要的认证字段。

认证字段可以按照下述步骤生成，首先采用如 MD5 的摘要算法计算上述其它字段的摘要，然后采用如 3DES 的加密算法，使用由视频提供装置事先唯一分配的对应于该短消息生成装置 12 的保密认证密钥对所计算的摘要进行加密，从而生成认证字段。

在此，也可以将认证字段之外的其它字段加密，从而使用户所发出的请求消息更加安全可靠。此时，认证字段可以是通过对上述加密的其它各字段计算摘要、并使用保密认证密钥加密得到的字段。

接着，在步骤 SP2，由短消息发送和接收装置 14 将该具有认证功能的请求短消息发送给提供视频点播服务一方的请求短消息处理装置 15。

接下来，在步骤 SP3，请求短消息处理装置 15 接收短消息发送和接收装置 14 所发送的请求短消息，对收到的请求短消息进行处理，提取用户身份识别符等有关节目的信息，并通过认证字段验证用户是否合法。

用户是否合法可以通过如下步骤来进行验证。首先采用如 MD5 的摘要算法计算所提取的所述用户身份识别符字段、节目识别符字段、格式识别符字段、请求时间字段、和播放时间字段的摘要。然后，采用如 3DES 的加密算法，使用由视频提供装置 16 唯一对应分配给用户端的短消息生成装置 12

的保密认证密钥对所计算的摘要进行加密、从而生成请求短消息中的认证字段，接着校验所计算的认证字段与收到的认证字段是否一致。

如果两者一致，则在步骤 SP4 中，判断发送该请求短消息的用户为合法用户。如果两者不一致，则表明该用户为非法用户，处理前进到步骤 SP11，请求短消息处理装置 15 记录该不合法用户并结束处理。

如果在步骤 SP4 中确认发出请求短消息的用户为合法用户，则处理前进到步骤 SP5，判断用户所点播的节目是否需要加密。

如果在步骤 SP5 中确定用户所点播的节目需要加密，则处理前进到步骤 SP6。在步骤 SP6 中判断用户所点播的节目是否通过有条件接入系统发送。如果不是通过有条件接入系统发送的，则必须在步骤 SP8 中生成至少包含加密该节目内容的加密密钥在内的应答消息，并发送到用户端的短消息发送和接收装置 14，然后提供给节目播放装置 13，以便在播放节目时，使用该加密密钥对收到的加密节目内容进行解密。

如果在步骤 SP5 中确定用户所点播的节目无须加密，以及在步骤 SP6 中确定用户所点播的节目是通过有条件接入系统发送的，则处理前进到步骤 SP7，判断是否需要向用户端发送应答消息。

也就是说，此时，如果用户所点播的节目无须加密，则不用发送加密密钥；并且，虽然用户所点播的节目内容是加密的，但是该加密内容是通过有条件接入系统发送的，也无须通过请求短消息处理装置 15 向用户端发送加密密钥，而是可以通过有条件接入系统的专用信道向节目播放装置 13 直接发送。

如果在步骤 SP7 中确定需要向用户端发送一确认消息，即表明收到用户请求的确认消息，则在步骤 SP8 中生成该确认消息并发送给短消息发送和接收装置 14，通知用户已经收到其请求。

接着，在步骤 SP9，请求短消息处理装置 15 将所提取的有关用户点播的节目的信息提供给视频提供装置 16，视频提供装置 16 根据该节目信息，在合适的时间将节目识别符所对应的节目内容发送到用户身份识别符所指示的用户端。同时，在用户端的节目播放装置 13 接收视频提供装置所发送的节目。

以上结合附图描述了本发明的优选实施例，但是本发明并不仅限于该具体的实施方式。在不偏离权利要求的精神和范围的情况下，可以对其做出种种改变。

例如，短消息生成装置 12 和节目播放装置 13 可以用一个装置实现，并配置到传统的机顶盒中。

此外，上述图 5 流程图所示的方法不一定必须按照所叙述的顺序执行，并且可以跳过某些步骤。例如，请求短消息可以不加密，当然在提供视频点播服务一方的请求短消息处理装置也就无须对收到的请求短消息解密。

另外，根据本发明的视频点播方法也可以用计算机程序实现并记录在计算机可读的记录介质中，整个系统也可以借助于通用个人计算机来实现。

利用本发明的视频点播系统及其方法，不仅无需对现有通过有线电缆进行视频点播的系统进行双向改造，而且方便了那些没有因特网接入的用户。同时，其保密性也得到了保证，为运营商提供了良好的运行环境。

说 明 书 附 图

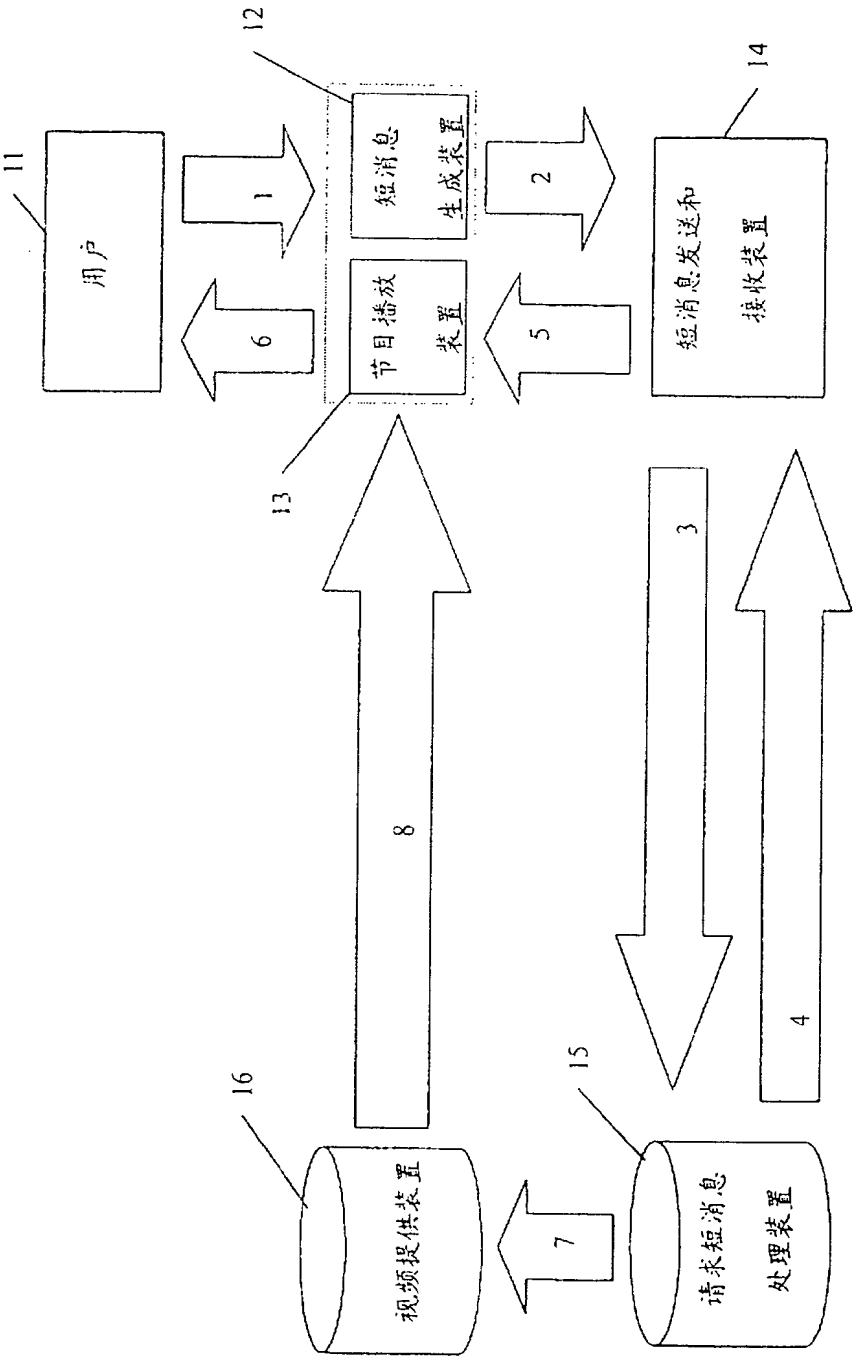
用户
11
短消息
生成装置
12
节目播放
装置
13
短消息发送和
接收装置
14
请求短消息
处理装置
15
视频提供装置
16
1
2
3
4
5
6
7
8

图 1

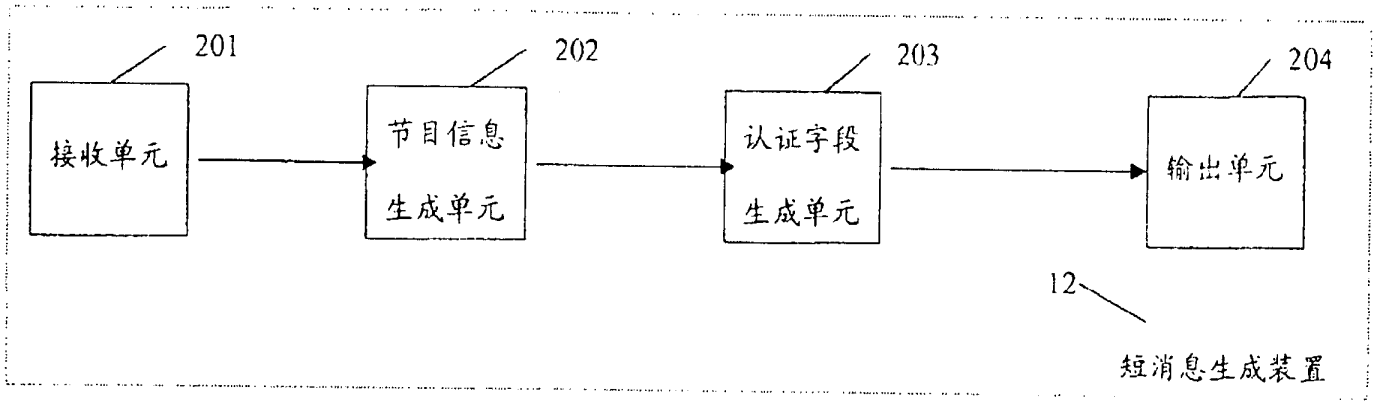

图 2

格式识别符字段	用户身份识别符字段	节目识别符字段	请求时间字段	播放时间字段	认证字段	可选字段

图 3

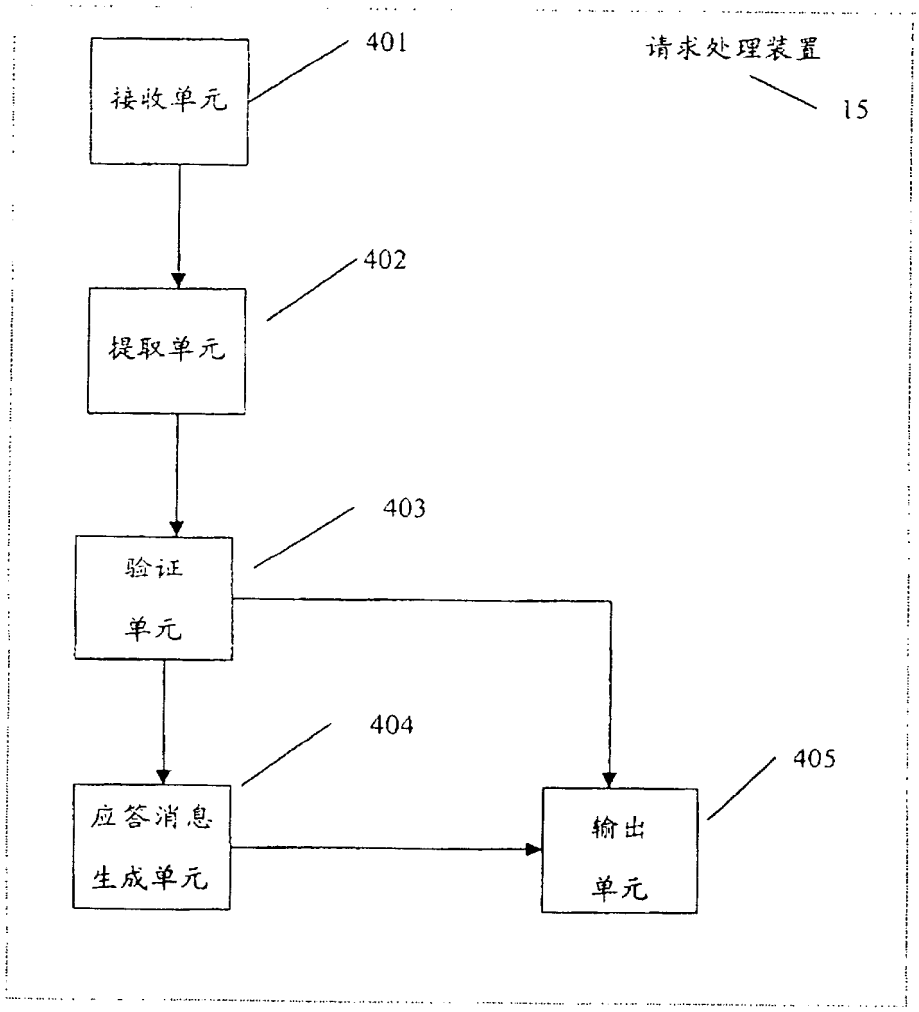

图 4

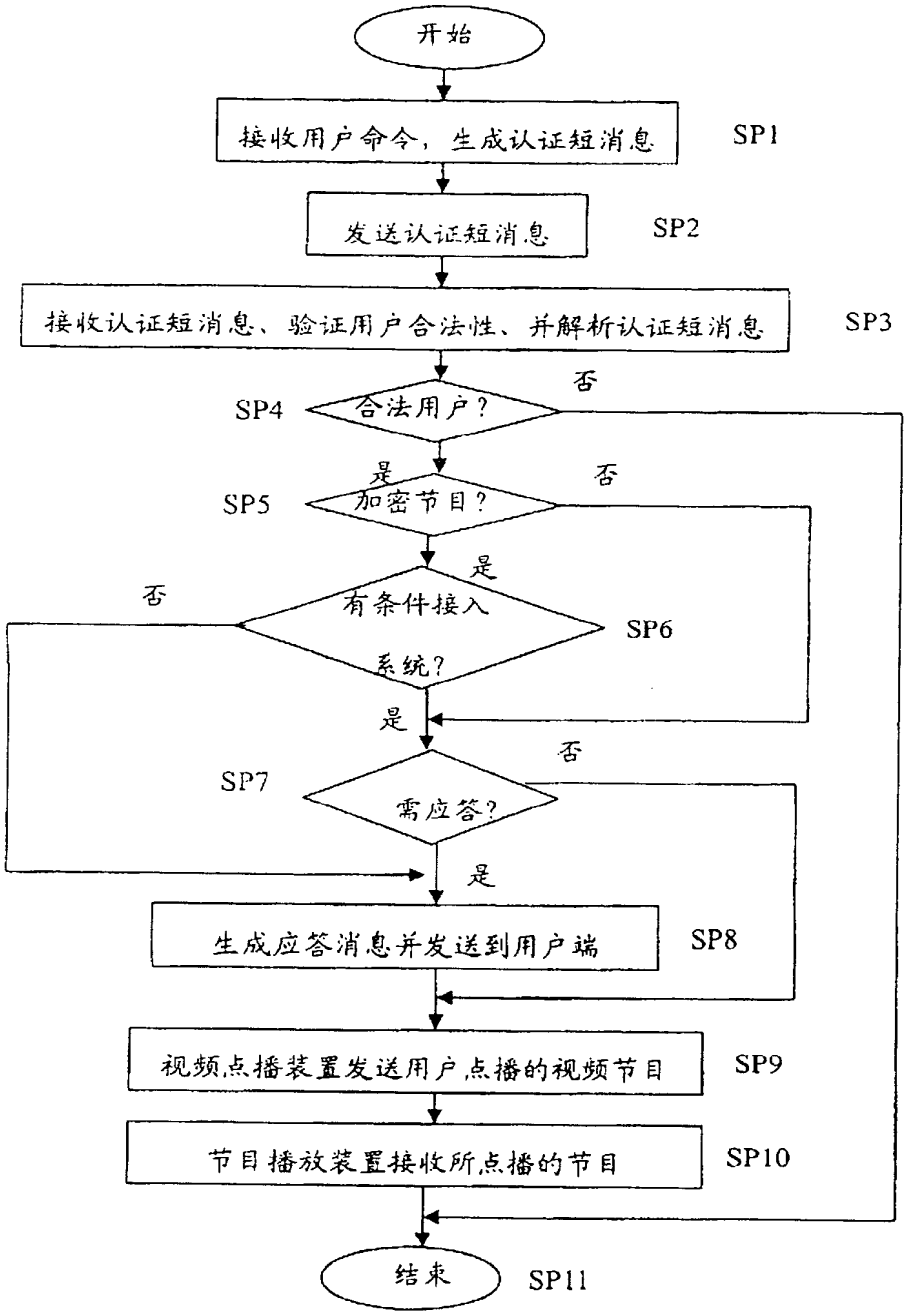
开始
接收用户命令，生成认证短消息
SP1
发送认证短消息
SP2
接收认证短消息、验证用户合法性、并解析认证短消息
SP3
SP4
合法用户？
否
是
SP5
加密节目？
否
是
否
有条件接入系统？
SP6
是
SP7
需应答？
否
是
生成应答消息并发送到用户端
SP8
视频点播装置发送用户点播的视频节目
SP9
节目播放装置接收所点播的节目
SP10
结束
SP11

图 5